www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Integration Strategy of Cyber Defense with National Cyber Security to Maintain State Sovereignty

Andi Sutomo[1], Amarulla Octavian[2], Pujo Widodo[3], Yono Reksoprodjo[4]
[1,2,3,4]*Universitas Pertahanan Indonesia*
andi.sutomo@idu.ac.id, amarulla.octavian@idu.ac.id, pujowidodo78@gmail.com, yono.reksoprodjo@kkip.go.id

Abstract

Threats to state sovereignty are becoming increasingly complex as technology develops rapidly. In order to overcome this incident, a national cyber system is needed which consists of cyber security, cyber defense, and other types of cyber with their main duties and functions in practice, preventive measures, prosecution, and so on to law enforcement as an effort to protect cyber ecosystems and assets. Vital from attacks through cyberspace (cyber attacks) that aim to disrupt the confidentiality, integrity, authentication, and availability of data and information. The paradigm of national security which has shifted to become more complex, including guaranteeing the privacy of every citizen, encourages the main obligation of a country to provide privacy protection from cyber-attack. The qualitative approach method used in this research is explanatory qualitative. The data used in this research is secondary data in the form of a literature study, by looking for various literature that is in accordance with the discussion on Strategy for Integration of Cyber Defense with Cyber Security Nationally to Maintain State Sovereignty. The current condition of cyber defense can be described based on aspects of Policy, Institutions, Technology and supporting infrastructure, and Human Resources (HR).

Keywords
Strategy; cyber defense; national cyber security

I. Introduction

Threats to state sovereignty are becoming increasingly complex as technology develops rapidly. This threat is not only conventional but also unconventional but still has a significant impact. One of them is the threat that arises from cyberspace regardless of distance, time, and national borders. In the cyber world, there are several terms and groupings, such as cyber warfare, cyber attack, cyber security, cyber defense, cybercrime, cyber threat, and so on.

Cyberspace has become a new unlimited war mandala in today's modern era where the source of the threat is not easy to guess whether it comes from individuals, countries, or individuals ridden by the state. Cyber-attacks have the potential to take access to owned assets, prominent incidents include identity theft and data (information resources) and account hijacking, cases of spreading viruses inserted in files and websites as well as important code, slander, blasphemy, or defamation. Apart from that, it can also take the form of industrial espionage and hostage-taking of critical information resources, this condition creates anxiety because of the loss of privacy as a result of the theft of important data and information related to state sovereignty.

Several small-scale cyber-attacks that occurred in several countries between the 1990s and 2012 include Internet social engineering attacks, Network sniffers, Packet spoofing, Hijacking sessions, Automated probes and scans, GUI (Graphical User Interface)

DOI: *https://doi.org/10.33258/birci.v5i1.3727*

intruder tools, Automated widespread attacks, Widespread denial-of-service attacks, Executable code attacks (against browsers), Techniques to analyze code with Vulnerabilities without source, Widespread attacks on DNS infrastructure, Widespread attacks using NNTP to distribute attack, "Stealth" and other advanced scanning techniques, Windows-based remote-controllable Trojans (Back Orifice), Email propagation of malicious code, Wide-scale Trojan distribution, Distributed attack tools, Distributed Denial of service (DDoS) attacks, Targeting of specific users, Anti forensic techniques, Wide-scale use of worms, dan Sophisticated command, and control attacks (Soewardi, 2013).

To overcome the above incidents, cyber security is needed which consists of various practices, preventive measures, and law enforcement as an effort to protect the cyber ecosystem and vital assets from cyber attacks that aim to disrupt the confidentiality, integrity, and availability of information or data (Fischer, 2005; IT, 2012). The assets in question are not limited to connect computing, including vital infrastructure, servers, networks, and information stored or transmitted via the internet. Interaction in Cyberspace can run well if it is supported by the availability, integrity, and confidentiality of information. Minor disturbances to system performance can cause significant economic losses (Kovacevic & Nikolic, 2015; Tabansky, 2011).

The national security paradigm that has shifted to become more complex, including guaranteeing the privacy of every citizen, encourages the presence of the state in providing privacy protection from cyber-attack. According to BSSN data at the cyber security operations center, there were around 741,441,648 cyberattacks in Indonesia, the data was from January to July 2021 and the highest number of cyber attacks occurred in May 2021, which was 186,202,637 attacks (idxchannel.com, BSSN, 2021). From these data, it can be said that the use of information and communication technology is directly proportional to the risk of security threats that can be obtained, this is what all of us need to pay attention to in securing national cyberspace, including the National Cyber and Crypto Agency (BSSN). So the disclosure of information and the connectivity of the internet network around the world in addition to providing convenience and benefits, but also has a negative impact on the country, including the privacy of every citizen.

The number of cyberattacks continues to increase quite drastically from time to time, from the observations of the most anomaly categories namely malware, denial of service, and trojan-activity while the trend is in the form of ransomware or malware attacks with the motive of encrypting data and then leading to a ransom request, followed by data leaks or data leaks. This cyberattack that occurred in Indonesia has the potential to harm the country's economy by 3.7 percent of the total Gross Domestic Product, which is USD 34.2 billion or equivalent to Rp. 481 trillion. This shows that Indonesia needs to make a breakthrough to protect important data and information owned by the state in the form of cooperation, synergy, and integration of cyber systems on a national scale.

The world health agency (WHO) has also announced that the corona virus, also called COVID-19, is a global threat worldwide. The outbreak of this virus has an impact especially on the economy of a nation and globally. These unforeseen circumstances automatically revised a scenario that was arranged in predicting an increase in the global economy. (Ningrum, P. et al. 2020)

The Covid-19 pandemic caused everyone to behave beyond normal limits as usual. One of the behaviors that can change is deciding the decision to choose a college. The problem that occurs in private universities during covid 19 is the decrease in the number of prospective students who come to campus to get information or register directly to choose the department they want. (Sihombing, E and Nasib, 2020)

The increase in the number of cyberattacks was also driven by the outbreak of the Covid-19 pandemic that hit most countries in the world, where this condition had a significant impact on various aspects of human life, ranging from ideology, politics, economy, socio-culture, as well as defense and security. This critical situation that arises is widely used by certain parties or individuals to commit cybercrimes, such as phishing (deception), theft of important data and information, as well as significant spams and ransomware attacks. It was further explained that the most cyberattacks were aimed at the government sector (45.5 percent), followed by the financial sector (21.8 percent), telecommunications (10.4 percent), law enforcement and transportation (10.1 percent), and Other SOEs amounted to 2.1 percent (committee.id, BSSN, 2021). This then triggers the emergence of strong pressure from various parties, such as the industrial, economic, university, defense, and security sectors, and so on so that the government immediately takes strategic steps to optimize existing potential and establish a national-scale Cyber System to protect critical information infrastructure.

Figure 1. *January-August 2019/2020 Number of Cyber Attacks (Pusat Keamanan Siber Nasional)*

The losses caused by cyber-attacks are largely determined by the characteristics of the target of the attack. For corporations, losses in the economic field such as reduced profits, loss of market value, lawsuits, and damage to reputation. For individual victims, the losses caused have an impact on psychological conditions and trigger stress, besides that, they also lose privacy and financial losses. Cyber threats (cyber-threats) that have the potential to cause serious problems for networks and computer systems encourage an integration strategy of cyber defense with cyber security in national cyberspace to facilitate coordination and cooperation while still guided by the main tasks and functions of each stakeholder. In protecting critical information infrastructure and safeguarding state sovereignty.

II. Review of Literature

2.1. Cyber Defense

In the state, the defense aspect is a very fundamental factor in ensuring the survival of every nation and state. The defense of the Indonesian state is mandated by Law Number 3 of 2002 Article 1 Paragraph (1) concerning National Defense which is defined as "all efforts to defend the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia (NKRI), and the safety of the entire nation from threats and disturbances to the integrity of the nation and state". This mandate is further explained in Law (UU) Number 34 of 2004 concerning the Indonesian National Armed Forces Article 1 Paragraph (5) which states that the national defense is prepared by taking into account the geographical conditions of Indonesia as an archipelagic country. This is carried out in the context of realizing a universal national defense system. This means that the Indonesian state defense system involves all citizens, territories, and other national resources, and is prepared early by the government, and is carried out in a total, integrated, directed, and continuous manner to uphold state sovereignty, territorial integrity, and the safety of the entire nation from all kinds of threats.

2.2 National Cyber Security

Indonesia can currently be categorized as an emergency regarding cyber security, which is also known as cyber security. Realizing that the level of crime in cyberspace or cybercrime in Indonesia has reached an alarming level. According to the Ministry of Defense in the Minister of Defense No. 82 of 2014 concerning Guidelines for Cyber Defense, it is explained that National Cyber Security is all efforts in order to maintain the confidentiality, integrity, and availability of information and all supporting facilities at the national level, which are cross-sectoral. According to Fischer (2009), the notion of Cyber Security can be concluded as a series of activities and measurements intended to protect oneself from attacks, disruptions, or other threats through elements of cyberspace (hardware, software, computer networks). Cybersecurity can be described on the one hand as the policies, guidelines, processes, and actions necessary for electronic transactions to be carried out with the minimum risk of breach, intrusion, or theft. And on the other hand, cybersecurity is a tool, technique, or process used to protect information system assets.

The cyber component consists of soft and hard infrastructure, the soft infrastructure component consists of human resource managers and policymakers (people), policies, processes, protocols, and guidelines that create a protective environment to maintain systems and data (process), while the hard infrastructure is a technology consisting of hardware and software, needed to protect systems and data from external and internal cyber threats.

2.3 State Sovereignty

The sovereignty of a country over its territory is fundamental as one of the conditions in the state. The sovereignty of a country is very necessary so that other countries do not arbitrarily enter the territory of another country's sovereignty. State sovereignty emerged simultaneously with the establishment of the state. The concept of sovereignty is concerned with the relationship between political power and other forms of authority. Sovereignty can be understood by observing that: first, political power is different from the organizational framework or other authorities in society such as religious, familial, and economic; second, sovereignty asserts that this kind of public authority is autonomous and very broad (autonomous and preeminent) so that it is superior to existing institutions in the

society concerned and independent or free from outside parties. In international law, state sovereignty and equality between countries are concepts that are recognized and form the basis for the operation of the international legal system. International law has traditionally recognized that the state is an independent and sovereign entity, meaning that the state is not subject to another more powerful authority (Marcos, 2003: 1).

III. Research Methods

The qualitative approach used in this study is based on non-numeric data that can be in the form of text and images, and filtering of the data is carried out to make interpretations of the literature review (Creswell, 2003).

The qualitative approach method used in this research is explanatory qualitative to find out what and how the phenomena that occur between the research variables (Bandur. 2016). The data used in this research is secondary data in the form of a literature study. The literature study was carried out by searching for various literature that matched the discussion on Strategy for Integration of Cyber Defense with Cyber Security into a National Cyber System to Maintain State Sovereignty, especially protecting the country's critical information infrastructure.

IV. Research Method

4.1 Cyber Threats to State Sovereignty

Cyber threats and disturbances are closely related to the use of computer technology and internet networks. These cyber-threats can be grouped into several forms depending on the method used, such as Cyber Espionage, Cyber Warfare, Cyber Crime, and Cyber Terrorism (Sutedja, 2015). Cyber attacks are all forms of actions, words, or thoughts, whether intentional or not, by a party, with any motive and purpose, carried out anywhere, with the target of a system, electronic system, or content (information) or device that rely on technology and networks of various sizes, on material or non-critical objects that have military and non-military interests, which threaten state sovereignty, territorial integrity, and national security. Cyber attacks in the digital era are a challenge for many stakeholders. In the Minister of Defense Regulation No. 82 of 2014 it is explained that the types of cyber threats can be categorized into 3 groups, namely:

a. Hardware threats, namely threats caused by the installation of certain equipment in a system, so that the equipment can interfere with network systems and other hardware, for example, Jamming and Network Intrusion.
b. Software threats, namely threats by the entry of certain software to carry out activities such as Information Theft (Information Theft), Information / System Destruction (Information / System Destruction), Information Corruption (Information Manipulation), and so on, into a system.
c. Data/Information Threat (data/information threat), is a threat resulting from the dissemination of certain data/information, such as propaganda and information warfare.

Cyber threats have the potential to cause serious problems on a network or computer system and can affect anyone. For example, in the state domain, computer components are part of critical government infrastructure and are highly vulnerable to hackers and cyberattack targets. Minor disturbances in the operation of the system can cause significant economic losses (Kovacevic & Nikolic, 2015; Tabansky, 2011). For entrepreneurs, intellectual property theft, as well as security and data breaches, are common threats that

need to be addressed. At the same time, for each domain, one should be aware of the risks associated with data theft and the spread of malware and viruses (Bendovski, 2015).

4.2. Condition of Cyber Defense and National Cyber Security System in Indonesia

a. Cyber Defense

Cyber Defense is an effort to overcome cyber-attacks that disrupt the implementation of national defense (Cyber Defense Guidelines, 2014). The current state of cyber defense can be described as follows:

1) Policy

   Cyber defense policies complement existing policies regarding the development and use of information technology within the ministry in general. One of the policies that have become the basis for this is the Minister of Defense Regulation No. 16 of 2010 concerning the Organization and Work Procedure of the Ministry of Defense, one of which outlines the role of the Ministry of Defense's Center for Data and Information and Datin Units in the Ministry of Defense's Satker. In addition, the policies needed to support cyber defense have also been drawn up which will serve as a reference for the preparation, development, training, and operation of cyber defense. Laws and regulations related to cybersecurity in Indonesia divide responsibilities between several ministries and are considered ineffective in preventing cyber threats and crimes. Therefore, comprehensive regulations on network security are urgently needed in Indonesia. Cyber Defense is an effort to overcome cyber-attacks that disrupt the implementation of national defense (Cyber Defense Guidelines, 2014). The current state of cyber defense can be described as follows:

2) Institutional

   The institutions that are built must be by the needs of the implementation of cyber defense, to ensure that the objectives of cyber defense can be achieved optimally. The government's efforts to organize the national cyber system already exist and deserve to be appreciated, including the entrusting of the National Crypto Agency (Lemsaneg) to coordinate the national cyber system so that the institution changed its name to the National Cyber and Crypto Agency (BSSN). The President of the Republic of Indonesia as the head of state has confirmed BSSN as an institution responsible for the cyber field with the task of carrying out cyber tasks effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security so that the duties and responsibilities that must be carried out by BSSN are very clear. . Considering the urgency of the tasks that must be carried out by this institution, while the existing cyber elements are quite varied according to the field of duty of each Ministry/Agency, awareness is needed from all parties that the task is quite heavy so it is necessary to build good cooperation, integration, and interoperability.

3) Technology and supporting infrastructure

   The currently available technology, both general and specifically to support cyber defense, is still in the process of being improved. Meanwhile, the required technology/infrastructure support includes: (1) building infrastructure/data center location, NOC, laboratory, and other supporting facilities; (2) Data Center and Recovery Center (DRC); (3) Data network; (4) cyber defense administration applications; (5) special cyber defense technical applications; and (6) special technology (hardware and software supporting specific cyber defense activities).

   The cyber defense infrastructure that has been deployed at the Ministry of Defense and the TNI has been operating well, although there are still some obstacles and limitations, including the equipment that is getting old, including the technology it uses, which is

increasingly lagging when compared to the development of information and communication technology which is so advanced and rapid. so that strategic steps are needed to continue to develop it, whether it is in the form of upgrading both software and hardware including human resources or it can also be rejuvenating all existing cyber equipment but this is also very much determined by the state's financial condition.

4) Human Resources (HR)
The main asset in cyber security is personnel or human resources who play a very important role in cyber defense. Preparations for the provision of human resources to support cyber defense have already begun, although this is only the initial preparation in the form of an awareness-raising program and an increase in information security knowledge and skills (Pedoman Pertahanan Siber, 2014).

b. National Cyber Security

National Cyber Security is all efforts to maintain the confidentiality, integrity, and availability of information and all supporting facilities at the national level, which are cross-sectoral (Cyber Defense Guidelines, 2014). In general, cyber security is the process of protecting data, systems, networks, and programs from the threat of digital attacks. Cyber Security is also referred to as actions taken by users to protect computer systems from attacks or illegal access by irresponsible parties with various methods. Either access sensitive information and steal it, as well as alter and destroy important data. Various motives behind the cyber-attack, both from political elements, business competition, and extortion of money (Rumi, Without Years).

Indonesia's cybersecurity is currently in a dangerous and critical stage. This is due to the increasing global information traffic that passes through and enters the Indonesian national information network system. Indonesia is in the first position to become a target for hackers to replace China, triggering the flow of information that is increasingly difficult to control. This situation encourages global cybercrime which has the potential to paralyze national information systems if not controlled (Arianto & Anggraini, 2019).

Regulations regarding national cyber security in Indonesia are Law Number 11 of 2008 concerning Information and Electronic Transactions, Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Information Technology Number 4 of 2016 concerning Information Security Management Systems, and Regulation of the Minister of Communication and Information Technology Number 29/PER/M.KOMINFO/12/2010 which is an amendment to the Regulation of the Minister of Communication and Information Technology No.16/PER/M.KOMINFO/10/2010 and is a revision of the Regulation of the Minister of Communication and Information Technology No. 26/PER/M.KOMINFO/5/2007 concerning Security of Internet Protocol-Based Telecommunication Network Utilization. This regulation forms the basis for the Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII) which is assigned to:

Several organizations that also work sectorally in dealing with cybercrime, include Information and Communication Technology Council (TIK Council), Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC), Indonesia Computer Emergency Response Team (ID-CERT), Computer Security Incident Response Team (CSIRT), Indonesia Telecommunications User Group (IDTUG). The organizations mentioned above also contribute to dealing with cybercrime but do not focus on Indonesia's national interests.

Another international standard is the NIST Cybersecurity Framework. The NIST Cybersecurity Framework provides a computer security policy framework for guidance on how private sector organizations in the United States can evaluate and improve their ability to prevent, detect, and respond to cyber-attack threats.

Currently, the cyber security system in Indonesia is still not effective, several problems are faced in the development of national cyber security, including:

a. Weak state understanding of cyber security which requires service restrictions where servers are located overseas and require the use of a secured system;
b. Legality of handling attacks in cyberspace;
c. The pattern of cybercrime occurrences is so fast that it is difficult to deal with;
d. National Cyber Security institutional governance;
e. Low awareness of the threat of international cyberattack that can paralyze a country's vital infrastructure; and
f. The weakness of the domestic industry that produces and develops hardware or hardware related to information technology is a gap that can weaken defenses in cyberspace (Arianto & Anggraini, 2019).

To deal with these conditions, the cyber defense which has been the domain of the Ministry of Defense and the TNI must also make improvements and transformations so that they can synergize both internally and externally against the real threats facing the state. The efforts of cyber elements that include many Ministries/Agencies to work together, synergistically, and together are consistent with their respective activity domains, but in reality, these elements still operate independently. Indeed, many things make it difficult to build integration and interoperability, especially BSSN as the coordinator of network security has not received much attention because there are still other functions that are running. As a crypto organization, industry egos still dominate in every organization, and awareness of the importance of integration, collaboration, and interoperability remains thin. Several ministries and organizations already have the cyberinfrastructure, including the Coordinating Ministry for Political, Legal, and Security Affairs, the State Intelligence Agency (BIN), the Indonesian Ministry of Defense, the National Police, the Ministry of National Defense, and members of the TNI and their staff.

4.3. Strategy for Integration of Cyber Defense with Cyber Security Systems

In this digital era, technology plays a very important role. Computers and the Internet have become tools of everyday life, so every country must be able to control, direct, and monitor human movements in cyberspace. It is not enough to just focus on the technological aspects to solve cybersecurity problems. Cybersecurity must be an ecosystem where law, organization, skills, collaboration, and technical implementation work in harmony to be effective. Therefore, it is very important to promote a cybersecurity culture so that citizens have the awareness to participate in surveillance and recognize the risks of using electronic networks.

In the cyber world, several terms and groupings are known including Cyber Warfare, Cyberattacks, Cyber Security, Cyber Defense, Cyber Crime, and so on, which Surely all of them use the cyber world (virtual world) which makes the internet network a medium of movement. They are closely related to each other only when faced with the main tasks of each institution so that there is a dividing line between each domain. As an illustration, when a crime occurs in cyberspace, it is considered a Cyber Crime area which is the responsibility of the Police, because it is related to crime, it is necessary to enforce the law, so it is included in the Cyber Security category which involves many parties related to law enforcement. Given the large number of Cyber Attacks (attacks through cyberspace), what

is called Cyber Defense is needed so that we have the deterrence and ability to protect and defend the country's critical information infrastructure, even if necessary, we must be able to counterattack to stop attacks that occur done by the opposing party. If all of this cannot be managed properly then Cyber Warfare will occur.

Internationally, there is a general concept in tackling cyber-attacks, namely Global cyber-security. Global Cyber-security is based on five areas of work: First, the element of legal certainty (cyber-crime law). Second, technical factors and procedural actions (special actions in tackling cyber-attacks). Third, the organizational structure factor (organizations that play a role in cyber security). Fourth, the factor of capacity building and educating users (publicity campaigns and education about cyber security). Fifth, the element of international cooperation (including cooperation in efforts to overcome cyber threats) (Yanuar, 2021).

The cyber defense strategy that can be applied by Indonesia in dealing with cyber security threats can use five concepts applied by Global Cyber-security, including:

1. Legal certainty

   Regarding legal certainty. The development of cyber security is the availability of security policy documents, standard documents that are used as a reference in the implementation of all procedures related to information security. The development and strengthening of cyber security policies in Indonesia must be integrated into the national strategy for the development of the national cyber security ecosystem that has been prepared by the government. The National Strategy for Building a National Cyber Security Ecosystem prepared by the government includes legal efforts, technical efforts including standards and activities, organizational and institutional arrangements that carry out cyber security for the national interest, capacity building or capacity building of human resources (HR) in the cybersecurity sector and strengthening cooperation internationally (Ardiyanti, 2014).
2. Technical and procedural actions

   For this second element, actual technical and procedural actions are required from each cyber security actor related to information security. The key elements of cyber security that must be considered in the availability of information infrastructure are hardware and software. infrastructure standards must comply with international standards to deal with cyber threats, including an adequate full perimeter defense system, having a network monitoring system, network security assessment (Yanuar, 2021).
3. Organizational Structure

   Cyber threats are included in asymmetric threats where handling requires a holistic approach. Due to its multidimensional nature, ensuring cybersecurity is not only the task of one department but also many other departments that require a coordinating body.

   Strong national cyber institutional arrangements are one of the prerequisites for achieving reliable cyber security. Therefore, the establishment of regulations and institutional organizations that manage cyber security at the national level must be integrated. As a regulator, it can cooperate with the Directorate of Information Security (Kominfo), IDSIRTI (Indonesian security incident response team on internet infrastructure), and the state code agency. As law enforcers, they can cooperate with the police, the ministry of law and human rights, the attorney general's office, and the courts. In the defense/military aspect, it can cooperate with the ministry of defense and the TNI, while in the intelligence aspect, it can cooperate with the State Intelligence Agency (BIN) and the Strategic Intelligence Agency (BAIS).

4. *Capacity building*
   The limited mastery of technology is a major issue in the formulation of network security policies. Given the rapid development of technology, the management of cybersecurity resources must receive serious attention from all related aspects. This is necessary because cybersecurity is not something cheap and develops very quickly. By developing infrastructure capabilities by placing it as a business process, the potential losses or costs arising from technology development can be reduced. Likewise with the capacity development of human resources involved in cybersecurity. With the management of cyber security HR, it is hoped that it can accelerate the fulfillment of the needs of human resources who master the field of cyber security.
5. International Cooperation
   International cooperation related to the development of cyber-security is in the context of increasing the capacity of cyber security capabilities, both for infrastructure, facilities and in developing human resources in the field of cyber-security, both bilaterally between two countries as well as regionally or internationally. Increased cooperation in the field of information technology and cyber security is also expected to open up opportunities for the development of the media industry related to new information technology in Indonesia as part of the sector development strategy (Ardiyanti, 2014).

The strategy of integrating cyber defense with national cyber security can also be realized using the Ends, Means, and Ways strategies, namely:

Ends, what's secured? In building the integration of cyber defense with national cyber security, what needs to be secured is the national interest, including in this case critical information infrastructure in the form of government, defense and security sectors, banking, health, energy and human resources, transportation, information and communication technology, and food security.

Means, with what secure? To realize cyber defense integration by implementing a national security system, it can be implemented by conducting Quad helix cooperation between government, industry, academia, and the cyber community. In this case, the government plays a role in maintaining the national cyber environment, protecting national e-commerce, protecting national information infrastructure, controlling the penetration of ipoleksosbudhankam, and protecting citizens' privacy. Industry players can play a role in device development, software development, and network development. Academics can play a role in the application of science according to their respective majors, such as majoring in information systems, information technology, computer science, cyber, asymmetric warfare, etc. Cyber communities can build mutually supportive cooperation with government, industry, and academia, besides that they can also exchange ideas with fellow members of the cyber community, and build community communities that in the future can be useful in handling cyber threats.

Ways, how to secure? Layered, simultaneous, and parallel strategy, implementation of security management. Building synergies between industrial cyber control centers, special cyber community control centers, and academic cyber control centers, commanded by the government's cyber control center as the leading sector.

It is necessary to have rules of the game as a guide in its implementation and also to have a clear legal umbrella so that all stakeholders understand the duties and limits of the authority of each party so that they do not conflict with norms or legal rules that apply both internationally and nationally. For this reason, all parties need to equalize perceptions about the dangers and impacts arising from cyber attacks, threats, or attacks through cyberspace that can occur at any time regardless of distance, time, and national boundaries. Therefore, it is necessary to have a force that has special abilities to deal with these attacks.

Cyber power development needs to be done early on by involving all elements capable of carrying out cyber warfare.

Building cyber power is not an easy thing and definitely requires a fairly high cost to build it. The most appropriate strategy is how to consolidate all national cyber stakeholders, equalize perceptions of the dangers that can be caused in the event of a cyber attack, make maximum use of the existing infrastructure and have been deployed in several Ministries/Agencies and other institutions, build cooperation between government institutions, the private sector, and other organizations that have cyber capabilities. And what is no less important is that a legal umbrella is needed as a moving basis for all parties, institutions, or cyber elements in carrying out their duties.

The real condition now is that almost all cyber elements spread across several ministries/agencies and private sectors are still running independently and not well coordinated so that they give the impression of being individual and sectoral, this is one of the phenomena that need to be solved. Therefore, the BSSN which has been mandated by the government needs to take steps to invite all cyber elements to cooperate, build synergy, collaboration and interoperability in the hope that it will become a reliable national cyber system strength. This concept is the right solution considering the high costs involved in building a cyber system. By building good cooperation and synergy, Indonesia will have a strong national cyber system capability.

IV. Conclusion

Seeing the advancement of cyber technology around the world, Indonesia seems to be one of the most important actors in future cyber information traffic management. The integration of Cyber Defense with National Cyber Security to Maintain State Sovereignty has not been maximized because the national cyber security strategy is still constrained from the aspect of human resources, prevention, and security policies and procedures which still require coordination with all policymakers from the private sector, government, community, and foreign institutions that are developers of applications that are often used as media for cybercrimes, and technologies that must be developed in line with the increasing types of cyberattacks. Internationally, there is a general concept in tackling cyber-attacks, namely global cyber-security. Global Cyber-security is based on five areas of work, namely elements of legal certainty, technical factors and procedural actions, organizational structure, capacity building and educating users, and elements of international cooperation.

References

Andriyanti, H. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. Politica, 5(1), 95-110.

Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siber global melalui Indonesia security incident response team on internet infrastructure (ID-SIRTII). Jurnal Pertahanan & Bela Negara, 9(1), 13-29.

Badan Siber dan Sandi Negara. (April 2020). Rekap Serangan Siber (Januari-April 2020). Accessed via https://bssn.go.id/rekap-serangan-siber-januari-april-2020/, on January 1, 2022.

Bandur, A. (2016). Penelitian Kualitatif-Metodologi, Desain dan Teknik Analisis Data dengan Nvivo 11 Plus. Edisi Pertama. Jakarta: Mitra Wacana Media

Bendovschi, A. (2015). Cyber-attacks – trends, patterns, and security countermeasures. Procedia Economics and Finance. Doi: 10.1016/S2212-5671(15)01077-1.
Brownlie, Ian. 1990. Principles of Public International Law. Fourth Edition. Oxford: Clarendon Press.
Creswell, J. W. (2003). Research design: Qualitative, quantitative, and mixed methods approaches (2nd Ed.). Thousand Oaks, CA: Sage.
Fischer, E. A. (2009). Creating a National Framework for Cybersecurity: an Analysis of Issues and Options. New York: Nova Science Publishers, Inc.
Kementerian Pertahanan Republik Indonesia. (2014). Pedoman Pertahanan Siber.
Kovacevic, A., & Nikolic, D. (2015). Cyber-attacks on critical infrastructure: Review and challenges. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. Doi: 10.4018/978-1-4666-6324-4.ch001
Marcos, Miguel González. 2003. The Search for Common Democratic Standards through International Law. Washington: Heinrich Böll Foundation North America.
Mashabi, Sania. (2021). BSSN: Hingga Agustus 2021 Tercatat 888 Juta Serangan Siber. Kompas.com. https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber. Accessed January 1, 2022.
Ningrum, P. et al. (2020). The Potential of Poverty in the City of Palangka Raya: Study SMIs Affected Pandemic Covid 19. Budapest International Research and Critics Institute Journal (BIRCI-Journal). P. 1626-1634
Pellet, Alain. 2000. "State Sovereignty and the Protection of Fundamental Human Rights: an international law perspective". , Pugwash Occasional Papers, I: i: February 2000. http://www.pugwash.org/ publication/op/opv 1n1. Htm. [13 Juni 2021].
Peraturan menteri pertahanan nomor 82 tahun 2014 tentang pedoman pertahanan siber
Perpres Nomor 53 Tahun 2017 dibentuk Badan Siber dan Sandi Negara
Rumi, A. (No Year). Pengertian Cyber Security, Jenis Ancaman dan Manfaat untuk Pengguna. Pandagila.com. accessed via https://pandagila.com/pengertian-cyber-security-jenis-ancaman-dan-manfaat-untuk-pengguna/, on December 31, 2021.
Sihombing, E and Nasib, (2020). The Decision of Choosing Course in the Era of Covid 19 through the Telemarketing Program, Personal Selling and College Image. Budapest International Research and Critics Institute-Journal (BIRCI-Journal). P. 2843-2850.
Soewardi, B. A. (Maret 2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh bagi Indonesia. Media Informasi Ditjen Pothan Kemhan. Hlm.31-25.
Sutedja, A. (2015). Cyber Security & Pentingnya Dunia Usaha Memahaminya: Sebuah Pengantar. Indonesia Cyber Security Forum (ICSF)
Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara
Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia
UU Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 dan versi revisi UU ITE Nomor 19 Tahun 2016.
Yanuar, Adams Pratama. (2021). Cyber War: Ancaman Baru Keamanan Nasional dan Internasional (Cyber War: New National and International Security Threat). Jurnal Keamanan Nasional Volume VII, No. 1.